UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JAY KAY COLLISION CENTER, INC., individually and on behalf of all others similarly situated, Plaintiff, v. CDK GLOBAL, LLC, Defendant.	Case No. 1:24-cv-5313 Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff Jay Kay Collision Center, Inc. ("Plaintiff") brings this Class Action Complaint on behalf of itself and all others similarly situated, against Defendant CDK Global, LLC ("CDK" or "Defendant"), and alleges as follows.

NATURE OF THE ACTION

1. CDK provides management systems for more than 15,000 car dealerships, automobile repair centers, original equipment manufacturers, software vendors, and other service providers.

2. CDK's failures to implement reasonable data security caused a data breach, impacting the sensitive personally identifiable information of millions of consumers and disrupting the business operations of thousands of car dealerships, and automobile maintenance and repair services businesses that use or rely on CDK's software solutions to run their businesses (the "Data Breach").

3. CDK began to experience outages on June 18, 2024.

4. In response, CDK shut down its systems early on June 19, 2024. While CDK is assessing the overall impact of the data breach, nearly 15,000 dealerships and other businesses that rely on CDK's software programs and platforms have been left without much needed and bargained for services, such as being unable to process sales, perform maintenance and repair services, or complete other critical tasks for their office administration, documentation, and financing.

5. After CDK became aware that its systems were breached, CDK failed to safeguard its systems and CDK's computer systems were breached a second time on June 19, 2024. The cyberattack knocked out Defendant's systems for days, and adversely affected Plaintiff's and Class members' business processes. As of the filing of this Complaint, the outage is still in effect.

6. Plaintiff and Class members are automobile dealerships and services providers who were injured as a result of the Data Breach, and the disruption of Defendant's networks and services. Plaintiff and Class members seek damages and injunctive relief for the injuries they sustained as a result of the Data Breach, which continues to impact their businesses. The outage has caused a delay in critical business functions and disruption to businesses inflicting substantial costs to develop workarounds, and has potentially exposed their sensitive personal and financial information to criminals.

JURISDICTION AND VENUE

7. Venue is proper because Defendant resides in this District and a substantial part of the acts and omissions that form the basis of this Complaint occurred in this District.

8. Plaintiff is an Illinois corporation with its principal place of business in Chicago, Illinois.

9. Defendant is a Delaware corporation with its principal place of business in Hoffman Estates, Illinois.

10. The Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this case is brought as a class action, Plaintiff and Defendant are diverse parties, more than 100 members are in the putative Class, and the amount in controversy exceeds $5 million.

FACTUAL BACKGROUND

The Data Breach

11. The Data Breach involved two attacks that occurred on or around June 18 and 19, 2024, prompting Defendant to shut down its computer systems.

12. The Data Breach involved a ransomware attack. "When ransomware gangs breach corporate networks, they quietly spread to other devices while stealing corporate data. Once all data has been stolen and the threat actors gain administrative privileges, they encrypt all of the devices on the network, leaving behind ransom notes with instructions on contacting the hackers."[1]

13. The system outage that occurred starting on June 19, 2024, caused by the Data Breach, has slowed sales and forced auto dealerships and repair centers, and other businesses, to find alternative methods to order parts, and produce titles, contracts, leases, registration cards and other forms that must be delivered to customers, banks, and state departments of motor vehicles. Some have resorted to writing contracts by hand, or asking customers to wait days to take delivery of their vehicles. Vehicle services and repairs have hit a standstill in some cases because necessary parts cannot be ordered.

[1] https://www.bleepingcomputer.com/news/security/cdk-global-cyberattack-impacts-thousands-of-us-car-dealerships/

14. The shutdown has caused a massive disruption in the workflow of thousands of dealerships and automobile service centers throughout the nation.

15. According to an update provided by Defendant:

> If you are not aware, we experienced an additional cyber incident late in the evening on June 19.
>
> We continue to act out of caution, and to protect our customers, we have taken down most of our systems. Do not attempt to access the DMS until we can confirm the system is secure. Digital Retail and CDK phones continue to be functional.
>
> At this time, we do not have an estimated time frame for resolution and therefore our dealers' systems will not be available likely for several days.
>
> As of now, our Customer Care channels for support remain unavailable as a precautionary measure to maintain security. It is a high priority to reinstate these services as soon as possible.
>
> Along with the Critical Situation emails, we are providing updates in Unify and have two phone numbers to contact CDK for the latest recorded update. - CDK Global[2]

16. According to reports, the Data Breach was perpetrated by an Eastern European group known as Royal, or BlackSuit. The infiltration is reportedly carried out through what is known as a "callback phishing attack," where the target dials a phone number embedded in emails disguised as subscription renewals, and the attackers leverage social engineering tactics to trick the victims into installing remote access software and granting access to the targeted network.[3]

Defendant's Promises Regarding Data Security

17. At cdkglobal.com/infrastructure, CDK promises to "[e]nsure every line of communication and connection in your dealership is stable and secure" by taking steps to protect

[2] https://www.bleepingcomputer.com/news/security/cdk-global-hacked-again-while-recovering-from-first-cyberattack/

[3] https://www.bleepingcomputer.com/news/security/fbi-royal-ransomware-asked-350-victims-to-pay-275-million/

your customers and your business, avoid outages and downtime, and making sure every communication path is open and working efficiently.

18. Defendant states that "cybersecurity is a business priority."[4] Defendant advertised "peace of mind" with its three-tiered approach to protection against cyberattacks. Defendant purports to offer numerous cybersecurity features, including endpoint protection, network protection, security awareness training, mail protection, multifactor authentication and DealerComply, a service to help dealerships comply with data security regulations and laws.

19. Defendant promises to guard against ransomware and unsecured devices on your network with next-generation endpoint device monitoring and protection, among other things.[5] Defendant claims that its security features are robust enough that "you could hire a full-time internal team to handle network security. Or you could go with a more affordable option and get industry-leading threat intelligence with Endpoint Protect."

20. Defendant thus invited Plaintiff and Class members to put their trust in Defendant for supplying their data security needs and providing the assets, strategies, and personnel to manage their data security.

Defendant's Liability to Plaintiff and Class Members

21. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. Defendant knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

[4] https://www.cdkglobal.com/dealership-operations/cybersecurity
[5] *Id.*

22. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' personal and financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

23. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of the cyberattack, the risk of identity theft, and business interruption to Plaintiff and Class members has materialized and is present and continuing, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threats presented by the Data Breach; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of the services they were entitled to enjoy; and (e) the continued risk and disruptions to their business operations going forward while they implement changes and workarounds.

24. Plaintiff and Class members have spent and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching the Data Breach and Defendant's advisories and updates, and devising and implementing workarounds until the outage is safely rectified. For example:

- Celebrity Motor Car Company, a luxury car dealership reported to CBS MoneyWatch that its business was "completely shut down."[6] "We cannot process paperwork. Everything is frozen, everything is tied up—we cannot move money back and forth to pay off cars, to finance our customers' transactions."
- Geoff Pohanka told CBS News that his business, Pohanka Automotive Group is "very dependent upon the DMS, and it affects all parts of our business." "It generates all of our forms. If you come in, we enter you in the system, it builds a file in terms of paperwork and finance papers, and right now none of that is functioning."[7] While certain things can be accomplished by paper, the customer must come back to complete forms, and "everything takes longer [and] is more complicated."

25. Companies that provide automobile repairs and maintenance services use or rely on CDK software to order parts. Many parts orders cannot be completed while the outage is in effect, which delays the repairs.

26. Even large operations like Auto Nation said they are experiencing disruptions that are likely to negatively impact business.[8]

Plaintiff's Experiences

27. Plaintiff is unable to order parts due to the Data Breach, which causes delays in Plaintiff being able to repair automobiles. Only recently has Plaintiff been able to start ordering

[6] https://www.cbsnews.com/news/cdk-cyber-attack-outage-update-2024/
[7] *Id.*
[8] https://www.usatoday.com/story/money/cars/2024/06/24/cdk-cyber-attack-update/74191941007/

some, but not all, parts by calling in orders manually.

28. Plaintiff cannot check on the status of its pending parts orders, which also causes delays in repairing automobiles.

29. Plaintiff has to pay its employees to deal with the delays and business interruption caused by the Data Breach, and to spend time ordering parts manually.

30. The delay in repairing automobiles due to the Data Breach has adversely affected insurance company cycle times and rental car authorizations, and has delayed Plaintiff receiving payment for its repairs. Plaintiff gets paid after completing the repairs, and Plaintiff is delayed in being able to complete repairs due to an inability to get parts as a result of the Data Breach.

CLASS ACTION ALLEGATIONS

31. Plaintiff brings this action pursuant to the provisions of Fed. R. Civ. P. 23 on behalf of itself and the following Class:

> All persons and entities in the United States who used or relied on Defendant's services, and were injured as a result of the Data Breach.

32. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

33. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

34. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed Class is easily ascertainable.

35. Numerosity: Joinder of all Class members is impractical because Defendant serves more than 15,000 dealerships and other businesses nationwide, and Class members are geographically dispersed.

36. Commonality: Plaintiff and the Class members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and/or safeguarding the sensitive information targeted in the Data Breach;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to the Data Breach;

c. Whether the Defendant's security procedures and practices to protect its systems were reasonable in light of the measures publicly available and recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures facilitated, caused, and exacerbated the Data Breach;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members of the Data Breach;

g. Whether Defendant has or will adequately address and fix the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to prevent the Data Breach;

i. Whether Plaintiff and Class members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct.

37. Typicality: Plaintiff's claims are typical of Class members' claims. Plaintiff and Class members were uniformly impacted by the Data Breach, and sustained damages arising out of and caused by Defendant's common course of conduct in violation of law.

38. Adequacy of Representation: Plaintiff is an adequate Class representative. Plaintiff has the same interest in the litigation as the Class members, is committed to the prosecution and just resolution of this case, and has retained competent counsel who are experienced in conducting litigation of this nature.

39. Plaintiff is not subject to any individual defenses unique from those applicable to other Class members.

40. Superiority of Class Action: Since the damages suffered by individual Class members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought

or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

41. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

42. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class in its entirety.

43. Defendant's policies and practices challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

44. Unless a classwide injunction is issued, Defendant may continue failing to properly secure its systems, and Defendant may continue to act unlawfully as set forth in this Complaint.

45. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Plaintiff and the Nationwide Class)

46. Plaintiff re-alleges paragraphs 1–45 as if fully set forth herein.

47. At all times herein relevant, Defendant owed Plaintiff and Class members a duty of care to act with reasonable care to secure and safeguard their personal and financial information,

and to secure and safeguard its computer systems, and to use commercially reasonable methods to do so. Defendant took on this obligation upon itself by agreeing to provide Plaintiff and Class members, and provide vendors upon whom Plaintiff and Class members rely to operate their businesses, dealership management software and related services, and digitizing, aggregating, processing, and storing Plaintiff's and Class members' data in its computer networks.

48. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' data;

b. to protect Plaintiff's and Class members' data using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to secure and safeguard its computer systems using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

d. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

e. to promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their data and business operations.

49. Defendant knew that Plaintiff's and Class members' data was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

50. Defendant knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class members' data, the vulnerabilities of its data security systems, and the importance of adequate security. As a result of Defendant's knowledge about its ability to repel hackers that Plaintiff and Class members could not have known, and Defendant's public representations regarding its data security and privacy safeguards to the contrary, Defendant had a duty of care to disclose material facts of its susceptibility of attack, insufficient data security, and highly vulnerable systems critical to Plaintiff's and Class members' business operations.

51. Defendant knew about numerous, well-publicized data breaches.

52. Defendant knew and should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class members' data.

53. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect Plaintiff's and Class members' data.

54. Defendant breached duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' data.

55. Because Defendant knew that a breach of its systems could damage thousands of businesses, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the data contained therein.

56. Plaintiff's and Class members' willingness to entrust Defendant with their data was predicated on the understanding that Defendant would take adequate security precautions.

57. Moreover, only Defendant had the ability to protect its systems from attack. Thus, Defendant had a special relationship with Plaintiff and Class members.

58. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' data and promptly notify them about the Data Breach. These independent duties are untethered to any contract between Defendant and Plaintiff and Class members.

59. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

60. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class members have suffered damages and are at imminent risk of additional harms and damages.

61. To date, Defendant has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations and services obligations to Plaintiff and Class members.

62. Further, through Defendant's failure to provide clear notification of the Data Breach, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to mitigate the effects of the Data Breach.

63. The damages Plaintiff and Class members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

64. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class members have suffered and will suffer injury.

65. As a direct and proximate result of Defendant's negligent actions and negligent omissions, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, actual damages, loss of privacy, remedial and research expenses, costs to implement work-arounds and mitigate damages, loss of revenues and

sales, delays in payments and loss of use of funds, and other economic and non-economic losses.

COUNT TWO
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

66. Plaintiff re-alleges paragraphs 1–45 as if fully set forth herein.

67. Defendant offered to provide goods and services to Plaintiff and Class members in exchange for payment.

68. Defendant agreed that it would not disclose the Plaintiff's and Class members' information, and it would take reasonable steps to prevent a data breach.

69. Implicit in the parties' agreement was that Defendant would take reasonable measures to prevent foreseeable data breaches, would take expedient measures to limit the effects of the Data Breach, and would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access.

70. Plaintiff and Class members would not have entrusted their information to Defendant without such an agreement.

71. Defendant materially breached the contracts by failing to safeguard such information, failing to limit the Data Breach, and failing to provide prompt and accurate notice of the Data Breach.

72. As a direct result of the Data Breach, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, actual damages, loss of privacy, remedial and research expenses, costs to implement work-arounds and mitigate damages, loss of revenues and sales, delays in payments and loss of use of funds, and other economic and non-economic losses.

COUNT THREE
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

73. Plaintiff re-alleges paragraphs 1–45 as if fully set forth herein.

74. Defendant benefited from receiving Plaintiff's and Class members' payments and records by its ability to retain and use that information for its own benefit.

75. Defendant also understood and appreciated that Plaintiff's and Class members' information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

76. Plaintiff and Class members conferred a benefit upon Defendant by paying for its services, directly or indirectly, and in connection therewith, by providing their information to Defendant with the understanding that Defendant would implement and maintain reasonable data privacy and security practices and procedures. Plaintiff and Class members should have received adequate protection and data security.

77. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and appreciated the benefits.

78. Defendant failed to provide reasonable security, safeguards, and protections to the information of Plaintiff and Class members.

79. Defendant should not be permitted to retain money rightfully belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data security measures and caused the Data Breach.

80. Defendant accepted and wrongfully retained these benefits to the detriment of Plaintiff and Class members.

81. Defendant's enrichment at the expense of Plaintiff and Class members is and was unjust.

82. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class members seek restitution of their money paid to Defendant, and disgorgement of all profits and benefits, imposition of a constructive trust, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and all others similarly situated, requests that the Court enter judgment in Plaintiff's favor and against Defendant as follows:

A. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class and/or any other appropriate subclasses under Fed. R. Civ. P.23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

B. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

C. That the Court enjoin Defendant, ordering it to cease from unlawful activities;

D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

E. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members.

F. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

G. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

H. For all other Orders, findings, and determinations identified and sought in this Complaint.

Plaintiff Jay Kay Collision Center, Inc., individually and on behalf of all others similarly situated,

By: */s/ Thomas A. Zimmerman, Jr.*

Thomas A. Zimmerman, Jr. (IL #6231944)
tom@attorneyzim.com
Sharon A. Harris
sharon@attorneyzim.com
Matthew C. De Re
matt@attorneyzim.com
Jeffrey D. Blake
jeff@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
firm@attorneyzim.com

Marc E. Dann (*pro hac vice* anticipated)
Brian D Flick (*pro hac vice* anticipated)
DANNLAW
15000 Madison Avenue
Lakewood, Ohio 44107
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

Counsel for Plaintiff and the Proposed Class